Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (currently amended) A method for securing an accessible computer system, the method comprising:

receiving **[[a]]** more than one data packet that each includes a payload portion and an attribute portion and **[[is]]** are communicated between at least one access requestor and at least one access provider;

monitoring at least the payload portion of the data ~~packet~~ packets received by scanning the payload portion for at least one predetermined pattern and counting a number of data packets having payload portions that include the predetermined pattern; and

~~controlling~~ denying access by the access requestor to the access provider ~~when the payload portion is determined to include at least one predetermined pattern~~ when a number of payload portions that include the predetermined pattern exceed a configurable threshold number.

2. (cancelled).

3. (currently amended) The method as in claim 1 wherein monitoring the data ~~packet~~ packets includes scanning the payload portion while handling the data ~~packet~~ packets with a switch.

4. (currently amended) The method as in claim 3 wherein**[[:]]**

~~receiving the data packet includes receiving more than one data packet; and~~

monitoring the data packet includes monitoring only at least one data packet that is distinguished.

5. (currently amended) The method as in claim 1 wherein:

~~receiving the data packet includes receiving more than one data packet,~~

securing the accessible computer system further comprises distinguishing at least one of the data packets from among the data packets received for additional processing, and

monitoring the payload portion includes monitoring the payload portion of the at least one data packet distinguished.

6. (original) The method as in claim 5 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

7. (currently amended) The method as in claim 1 wherein**[[**:**]]**

~~receiving the data packet includes receiving more than one data packet; and~~

monitoring the data packet includes monitoring all of the data packets received.

8. (original) The method as in claim 1 wherein the access requestor is a client and the access provider is a host.

9. (currently amended) The method as in claim 8 wherein the data ~~packet is~~ packets are monitored when communicated from the client to the host.

10. (currently amended) The method as in claim 8 wherein the data ~~packet is~~ packets are monitored when communicated from the host to the client.

11. (original) The method as in claim 8 wherein the predetermined pattern includes a login failure message communicated from the host to the client.

12. (currently amended) The method as in claim 1 wherein the data ~~packet includes~~ packets include a token-based protocol packet.

13. (currently amended) The method as in claim 1 wherein the data ~~packet includes~~ packets include a TCP packet.

14. (currently amended) The method as in claim 1 wherein the data ~~packet includes~~ packets include a PPP packet.

15. (cancelled).

16. (currently amended) The method as in claim 1 wherein ~~controlling~~ denying access includes affecting bandwidth for communications between the access requestor and the access provider.

17. (currently amended) The method as in claim 1 ~~wherein controlling access includes~~ further comprising rerouting the access requestor.

18. (cancelled).

19. (currently amended) The method as in claim **[[**18**]]** 1 wherein ~~controlling~~ denying access by the access requestor to the access provider includes denying access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.

20. (currently amended) A system for securing an accessible computer system, comprising:

a receiving component that is structured and arranged to receive **[[a]]** more than one data packet that each includes a payload portion and an attribute portion and **[[is]]** are communicated between at least one access requestor and at least one access provider;

a monitoring component that is structured and arranged to monitor at least the payload portion of the data ~~packet~~ packets received and includes a scanning component that is structured and arranged to scan the payload portion for at least one predetermined pattern and to count a number of data packets having payload portions that include the predetermined pattern; and

an access controlling component that is structured and arranged to ~~control~~ deny access by the access requestor to the access provider when ~~the payload portion is determined to include at least one predetermined pattern~~ a number of payload portions that include the predetermined pattern exceed a configurable threshold number.

21. (cancelled).

22. (currently amended) The system of claim 20 wherein the monitoring component includes a scanning component that is structured and arranged to scan the payload portion while handling the data ~~packet~~ packets with a switch.

23. (currently amended) The system of claim 22 wherein**[[:]]**

~~the receiving component is structured and arranged to receive more than one data packet; and~~

the monitoring component is structured and arranged to monitor only at least one data packet that is distinguished.

24. (currently amended) The system of claim 20 wherein:

~~the receiving component is structured and arranged to receive more than one data packet,~~

the system further comprises a distinguishing component that is structured and arranged to distinguish at least one of the data packets from among the data packets received for additional processing, and

the monitoring component is structured and arranged to monitor the payload portion of the at least one data packet distinguished.

25. (original) The system of claim 24 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

26. (currently amended) The system of claim 20 wherein[[:]]

~~the receiving component is structured and arranged to receive more than one data packet; and~~

the monitoring component is structured and arranged to monitor all of the data packets received.

27. (original) The system of claim 20 wherein the access requestor is a client and the access provider is a host.

28. (currently amended) The system of claim 27 wherein the data ~~packet is~~ packets are monitored when communicated from the client to the host.

29. (currently amended) The system of claim 27 wherein the data ~~packet is~~ packets are monitored when communicated from the host to the client.

30. (original) The system of claim 27 wherein the predetermined pattern includes a login failure message communicated from the host to the client.

31. (currently amended) The system of claim 20 wherein the data ~~packet includes~~ packets include a token-based protocol packet.

32. (currently amended) The system of claim 20 wherein the data ~~packet includes~~ packets include a TCP packet.

33. (currently amended) The system of claim 20 wherein the data ~~packet includes~~ packets include a PPP packet.

34. (cancelled).

35. (original) The system of claim 20 wherein the access controlling component is structured and arranged to affect bandwidth for communications between the access requestor and the access provider.

36. (original) The system of claim 20 wherein the access controlling component is structured and arranged to reroute the access requestor.

37. (cancelled).

38. (currently amended) The system of claim **[[**37**]]** 20 wherein the access controlling component is structured and arranged to deny access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.

39. (currently amended) A computer program stored on a computer readable medium or a propagated signal for securing an accessible computer system, comprising:

a receiving code segment that causes the computer to receive [[a]] more than one data packet that each includes a payload portion and an attribute portion and [[is]] are communicated between at least one access requestor and at least one access provider;

a monitoring code segment that causes the computer to monitor at least the payload portion of the data ~~packet~~ packets received and includes a scanning code segment that causes the computer to scan the payload portion for at least one predetermined pattern and to count a number of data packets having payload portions that include the predetermined pattern; and

an access controlling code segment that causes the computer to ~~control~~ deny access by the access requestor to the access provider when ~~the payload portion is determined to include at least one predetermined pattern~~ a number of payload portions that include the predetermined pattern exceed a configurable threshold number.

40. (cancelled).

41. (currently amended) The computer program of claim 39 wherein the monitoring code segment includes a scanning code segment that causes the computer to scan the payload portion while handling the data ~~packet~~ packets with a switch.

42. (currently amended) The computer program of claim 41 wherein[[:]]

~~the receiving code segment causes the computer to receive more than one data packet; and~~

the monitoring code segment causes the computer to monitor only at least one data packet that is distinguished.

43. (currently amended) The computer program of claim 39 wherein:

~~the receiving code segment causes the computer to receive more than one data packet,~~

the computer program further comprises a distinguishing code segment that causes the computer to distinguish at least one of the data packets from among the data packets received for additional processing, and

the monitoring code segment causes the computer to monitor the payload portion of the at least one data packet distinguished.

44. (original) The computer program of claim 43 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

45. (currently amended) The computer program of claim 39 wherein[[:]]

~~the receiving code segment causes the computer to receive more than one data packet; and~~

the monitoring code segment causes the computer to monitor all of the data packets received.

46. (original) The computer program of claim 39 wherein the access requestor is a client and the access provider is a host.

47. (currently amended) The computer program of claim 46 wherein the data ~~packet is~~ packets are monitored when communicated from the client to the host.

48. (currently amended) The computer program of claim 46 wherein the data ~~packet is~~ packets are monitored when communicated from the host to the client.

49. (original) The computer program of claim 46 wherein the predetermined pattern includes a login failure message communicated from the host to the client.

50. (currently amended) The computer program of claim 39 wherein the data ~~packet includes~~ packets include a token-based protocol packet.

51. (currently amended) The computer program of claim 39 wherein the ~~packet includes~~ packets include a TCP packet.

52. (currently amended) The computer program of claim 39 wherein the data ~~packet includes~~ packets include a PPP packet.

53. (cancelled).

54. (original) The computer program of claim 39 wherein the access controlling code segment causes the computer to affect bandwidth for communications between the access requestor and the access provider.

55. (original) The computer program of claim 39 wherein the access controlling code segment causes the computer to reroute the access requestor.

56. (cancelled).

57. (currently amended) The computer program of claim [[56]] 39 wherein the access controlling code segment causes the computer to deny access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.